Development of a Process Assessment Model for Assessing Security of IT Networks Incorporating Medical Devices against ISO/IEC 15026-4

Anita Finnegan, Fergal Mc Caffery and Gerry Coleman
Regulated Software Research Group, Dundalk Institute of Technology & Lero, Dundalk, Co Louth, Ireland
{anita.finnegan, fergal.mccaffery, gerry.coleman}@dkit.ie

Keywords: Medical Device Security, Process Assessment, ISO/IEC 15026-2, ISO/IEC 15026-4, IEC 80001-2-2, IEC 62443-3-3, ISO/IEC 15504, ISO 27799, ISO/IEC 27001, ISO/IEC 27002.

Abstract: Advancements in medical device design over the last number of years have allowed medical device manufacturers to add more complex functionality particularly through the use of software. Such advancements include the ability for devices to communicate wirelessly across networks, from device to device and over the Internet. However, with such advancements comes additional risks; these are security risks, vulnerabilities and threats. In the past twelve months, concern within the medical device community has led to the US Government calling upon the FDA to take responsibility of medical device security. In support of this, this position paper details a research proposal to address medical device security issues through the development of a Process Reference Model (PRM) and a Process Assessment Model (PAM) to assess the capability of the processes used to develop medical devices intended to be incorporated onto healthcare networks and also determine the product security capability through the development of security assurance cases created following the lifecycle process. Further, in support of IEC 80001-2-2, the output from this PRM will be an assurance case with a security assurance level, which will be used to communicate the security capabilities of the product between Medical Device Manufacturers (MDMs) and Healthcare Delivery Organisations (HDOs). The intent is to build a better awareness of vulnerability types, threats and related risks to assist in reducing the likelihood of harm resulting from a security risk.

1 INTRODUCTION

Medical devices have made substantial innovative design improvements over the last number of years due to the growing incorporation of software in the devices. Following on from the addition of software came the introduction of interoperable medical devices bringing with it, a new set of security risks for consideration. Although there have been no reports of malicious attacks on interoperable medical devices, there have been quite a number of controlled hacking demonstrations. One such demonstration was at the Black Hat Security Conference in Las Vegas in 2011. A security researcher, Jeremy Radcliffe, manipulated the settings of his own insulin pump during a presentation. The ease with which the insulin pump was hacked created a lot of concern within the medical device community. Then in October 2012, Barnaby Jack, a researcher at IOActive, presented research results at the Breakpoint Conference in Australia, which looked at the security of pacemakers. Jack's research identified a bug in several manufacturers' pacemakers that allowed an attacker to deliver a potentially lethal shock to a patient's heart by sending a signal to the pacemaker by simply using a laptop. The pacemaker contained a coding error that allowed it to send a wireless command to the device that returned the model and serial number of the device.

Consequently, in a letter to the US Office of Management and Budget, the Information Security and Privacy Advisory Board (ISPAB) called upon the government to assign the responsibility of medical device security to a federal entity such as FDA. In August 2012, the Government Accountability Office (GAO) released a report of an audit carried out on the FDA for the assessment of two implantable medical devices that highlighted shortfalls in the assessment of intentional and unintentional risk (Government Accountability Office, 2012).

In addition to this quite a number of medical device security information and guidance documents

have been recently released. One example, the US Department of Homeland Security (DHS) issued a bulletin "Attack Surface: Healthcare and Public Health Sector"(DHS, 2012) which discusses security related risks associated with using medical devices on IT networks, including those risks to patient safety and theft or loss of medical information.

Addressing this recent concern, the aim of this research is to build security assurance into the product lifecycle through a set of strategic processes, activities and tasks and to establish and communicate the product security capabilities of a medical device between Medical Device Manufacturers, vendors and Healthcare Delivery Organisations. This will create awareness for both, the Medical Device Manufacturers in understanding the needs of the Healthcare Delivery Organisation, and also for Healthcare Delivery Organisation IT admin staff, to understand the capabilities of the medical device that could potentially be acquired for use on their IT network.

Section two of this paper outlines the most relevant standards and documents currently used within the software industry in relation to process assessment, software lifecycle assurance and security. Section three looks at related work in the area of process assessment models and security. Section four then discusses the future work planned for this research, including the validation of the model and also the impact this research is expected to have in the medical device domain for regulators, Medical Device Manufacturers, IT vendors and Healthcare Delivery Organisations.

2 CURRENT LANDSCAPE WITH STANDARDS

With the substantial transformation in medical device design over the last few years to incorporate software and communication functionality, the medical device communities around the world have published many standards and guidance documents to assist with the development of safe medical devices. This has resulted in an abundance of published security guidance documents and a sense of confusion among Medical Device Manufacturers and Healthcare Delivery Organisations with regards which guidelines and best practices to follow.

This section outlines the most applicable standards and guidance documents which are deemed most relevant in establishing and controlling security risks. A broad range of standards have been reviewed for this research, with the most fundamental being discussed here. Additional standards identified and incorporated into this research to date are discussed in Section three.

2.1 ISO/IEC 15026-4

ISO/IEC 15026-4 (IEEE, 2011) provides recommendations and guidelines for implementing software and systems development processes that require additional assurance for a particular property of that system or software; in this case the critical property is security. This standard presents a list of recommended processes, activities and tasks required in order to achieve a claim in relation to that critical property of a system or software. Through the development of an assurance case (further discussed in section 2.2), the entire development and maintenance of the product is addressed which also includes project-planning considerations. It is intended that this standard be used coupled with an already defined life cycle model.

2.2 ISO/IEC 15026-2

ISO/IEC 15026-2 (IEEE, 2011) defines requirements for the structure and content of an assurance case. An assurance case is a body of evidence organised into an argument demonstrating some claim that a system holds i.e. 'Is Assured'. An assurance case is needed when it is important to show that a system exhibits some complex property such as safety, security, or reliability (Goodenough et al., 2012).

A security assurance case is often compared with a legal case where there are two elements to the case, the argument and the evidence to support a claim. For an assurance case to be effective it must satisfy the following points:

- Must make a claim or set of claims about a property of a system;
- Provide a set of arguments;
- Make clear the assumptions and judgements underlying the arguments;
- Associate different viewpoints and levels of detail.
- Produce the supportive evidence;

2.3 IEC 80001-2-2

IEC 80001-2-2 (IEC, 2011c) is a technical report which provides a framework for the communication and disclosure of medical device needs, risks and controls which are to incorporated onto a IT

network. This technical report presents 20 security capabilities (Table 1) e.g. Authorization, Audit Controls etc. These capabilities provide Healthcare Delivery Organisations, Medical Device Manufacturers and IT vendors with information regarding user needs, security related requirements and required security control types.

This information is critical prior to development, acquisition, installation and use of medical devices for IT networks. Each of these security capabilities represents a potential security risk control. These are addressed in the requirement goals, which identify the risks that can be mitigated against through the use of that particular security capability. The user need section develops this further by detailing particular specific environmental requirements.

Table 1: IEC 80001-2-2 Security Capabilities.

	Security Capability	Code
1	Automatic Logoff	ALOF
2	Audit Controls	AUDT
3	Authorization	AUTH
4	Configuration of Security Features	CNFS
5	Cyber Security Product Upgrades	CSUP
6	Data Backup and Disaster Recovery	DTBK
7	Emergency Access	EMRG
8	Health Data De-Identification	DIDT
9	Health Data Integrity and Authentication	IGAU
10	Health Data Storage Confidentiality	STCF
11	Malware Detection/Protection	MLDP
12	Node Authentication	NAUT
13	Person Authentication	PAUT
14	Physical Locks on Device	PLOK
15	Security Guides	SGUD
16	System and Application Hardening	SAHD
17	Third-Party Components in Product Lifecycle Roadmaps	RDMP
18	Transmission Confidentiality	TXCF
19	Transmission Integrity	TXIG
20	Unique User ID	UUID

The security disclosure is a summary statement provided by the Medical Device Manufacturer and/or IT vendor that details the security capability of the medical device. This security disclosure is then reviewed by the Healthcare Delivery Organisation to establish the security integrity of the product and prompt further discussion prior to acquisition. The risk management team within the Healthcare Delivery Organisation utilise this further to perform a risk analysis based on the known security capabilities.

2.4 IEC 62443-3-3

IEC 62443-3-3 (IEC, 2011a) defines security system requirements based on a combination of system functional requirements and a risk assessment. Key inputs into the development of this document are security standards ISO/IEC 27002 (ISO/IEC, 2005) and NIST SP800-53(NIST, 2009). The standard is adopted by allowing the asset owner for the system so dictate the target Security Assurance Level (SAL-T). The standard details seven Foundational Requirements (FRs) as listed in Table 2. The seven FRs listed are the baseline for the system Security Assurance Levels (SALs). Within each of the seven FRs are applicable System Requirements (SRs). These are further broken down detailing the requirement of that SR, the rationale and supplemental guidance, the Requirement Enhancements (REs) and guidance for selection of REs relating to the SR dependent on the chosen SAL level for establishment of the achieved Security Assurance Level (SAL-A).

Table 2: IEC 62443-3-3 Foundational Requirements.

	Foundational Requirement	Code
1	Identification and Authentication Control	IAC
2	Use Control	UC
3	Data Integrity	DI
4	Data Confidentiality	DC
5	Restricted Data Flow	RDF
6	Timely Response to Events	TRE
7	Resource Availability	RA

3 SOLUTION DEVELOPMENT

3.1 Related Work

ISO/IEC 15504-2 (ISO/IEC, 2003) provides a measurement framework for process capabilities and defines the requirements for performing the assessment, building the Process Reference Model (PRMs), Process Assessment Models (PAMs) and verifying conformity of process models and the process assessment. Existing generic Software Process Improvement (SPI) models are available which include the Capability Maturity Model Integration (CMMI®) (SEI, 2010) and ISO 15504-5:2006 (ISO/IEC, 2006) (SPICE), but these models were not developed to provide sufficient coverage for regulatory compliance for the security of IT Networks incorporating medical devices.

While this relates to the development of the PRM

and the PAM for establishment of process assurance, it does not specifically address medical device product quality. One difference here is that, in addition to assessing the Medical Device Manufacturers software processes and practices, the key to this research is to also address product capabilities in relation to security of the interoperable medical devices.

To address the requirement for a PAM for assessing the security of IT networks incorporating medical devices, we undertook extensive research in this area assisted by leading members from the international standards IEC SC62A JWG7 working group looking at a medical devices specific SPI model. This work is being developed in collaboration with the SPICE User Group. The approach taken here is in line with the approach taken for both the development of Automotive SPICE (Automotive SIG) a domain specific SPI model for the automotive industry, and Medi SPICE (Fergal McCaffery and Dorling, 2010).

3.2 Proposal

ISO/IEC 15026-4 (IEC, 2011a) is a process lifecycle standard and provides a solid foundation for the PRM. It details processes for risk management which will be extended to include relevant security standards and requirements such as ISO/IEC 27002, ISO 27799 (ISO, 2008), IEC 62443, IEC 80001-2-2, NIST SP 800-53 and NIST SP 800-23 (NIST, 2009). All security controls and capabilities from these named sources will be crossed referenced and mapped to develop a comprehensive set of security capabilities which will need to be addressed when conducting a risk assessment and establishing relevant risk controls. For example, Automatic Log Off from IEC 80001-2-2 (Table 1) would use the requirements of SR.1.10 Session Lock in IEC 62443-3-3 as they relate to each other. All relevant controls/requirements from guidance docs and security standards included in the research will follow a similar mapping.

The PRM will provide a description of the processes and characterise these in terms of their purpose and outcome. This Process Assessment Model will be developed in compliance with ISO/IEC 15504-2 (ISO/IEC, 2003) which outlines what is required in the Process Assessment Model. This will be developed along with a measurement framework and ISO/TR 24774 (IEC, 2010) will provide the guidelines for process definition.

These steps take care of the processes to be addressed for the development of a product. Establishing process assurance or maturity has many benefits for both the medical device manufacturers and third party assessors in terms of meeting regulatory compliance and also determination of process quality. However, considering the security risks associated with interoperable medical devices consisting of software, a major objective is to establish a method for the communication of the final product quality in relation to security capabilities between the Medical Device Manufacturer, the IT vendor and the Healthcare Delivery Organisation. Communication of a security assurance level to Healthcare Delivery Organisations will provide a simple and meaningful method for establishing suitability of the device for the users need and its environment. To do this, IEC 62443-3-3 will be used as a guide for establishing the system security assurance level (SAL) by the Medical Device Manufacturers. The Healthcare Delivery Organisation will determine the appropriate security capabilities from within IEC 80001-2-2, along with any other validated capabilities from other standards. With regards the different types of SAL, the critical property is the achieved SAL (SAL-A) since this is most valuable to the Healthcare Delivery Organisation and FDA when establishing the security capability of the product. A SAL vector will be developed by the Medical Device Manufacturer post product development for the achieved SAL (SAL-A), which will be based on the target SAL (SAL-T) level (0-4) as determined by the Healthcare Delivery Organisation as the start of the acquisition process. The SAL vector that details the assurance level and security capabilities is presented here:

$$\text{SAL-A} = (\{\text{FR,}\}\ \text{domain}) = \{\text{AC}\ \ \text{UC}\ \ \text{DI}\ \ \text{DC}\ \ \text{RDF}\ \ \text{TRE}\ \ \text{RA}\}$$

$$\text{SAL-A} = (\{\text{FR,}\}\ \text{domain}) = \{3\ \ 3\ \ 3\ \ 3\ \ 2\ \ 1\ \ 0\}$$

For each of the parameters (refer to table 2 for FR descriptions) within the vector, a value of zero to four will be used to represent the SAL level for that particular requirement. Following on from this, the Medical Device Manufacturer will then verify the selected SAL level through the use of the SAL Mapping Matrix as shown in Annex B of IEC 62443-3-3 (IEC, 2011a), which will also be included in the PRM.

To further build upon the communication and disclosure of security capabilities, an assurance case, compliant with IEC/ISO 15026-2 (IEEE, 2011) will be developed by the Medical Device Manufacturer. Delivering the actual product assurance level will be achieved through the utilisation of a tool. This tool will be used for the development of the risk

assessment and will in turn automatically build the assurance case and outline in detail the evidence gathered to support the achievement of each SAL level.

The outcome of the PRM will be the development and communication of:
1. A process maturity level for the development of the product;
2. A security assurance case detailing in-depth the arguments and evidence supporting the security/safety claim of the medical device;
3. An achieved security assurance level (SAL-A) for the product.

4 SOLUTION DEVELOPMENT

It is planned that this model will be trialled in industry for validation purposes. This will be done at manufacturing facilities and Healthcare Delivery Organisations both in Ireland and the U.S. In addition to this, it is intended that the model will also be validated by experts from the International Standards Committee of IEC SC62A.

At present, there is much concern in the area of medical devices particularly related to security vulnerabilities, threats and risks of devices with communication abilities or those incorporated onto IT networks. Over the past 12 months, this concern has been highlighted through many federal body guidance publications and reports, security researchers' demonstrations, publications and also the development of new standards such as IEC 80001-1(IEC, 2011b).

With the publication of the GAO (Government Accountability Office, 2012) report in August, it is clearly indicated here that future strategies are required in order to sufficiently address medical device security. As medical devices become more advanced with software and complex wireless capabilities, it is feared that security vulnerabilities, threats and related risks will grow with this development. The GAO has recommended that the FDA work on addressing these issues following their assessment of FDA approved implantable defibrillators and insulin pumps.

IEC 80001-2-2 defines the security capabilities that a Medical Device Manufacturer or IT vendor must communicate to the Healthcare Delivery Organisation in order to enhance knowledge of security risks and controls the Healthcare Delivery Organisation IT admin staff should consider. This research sets out to support this from both a process

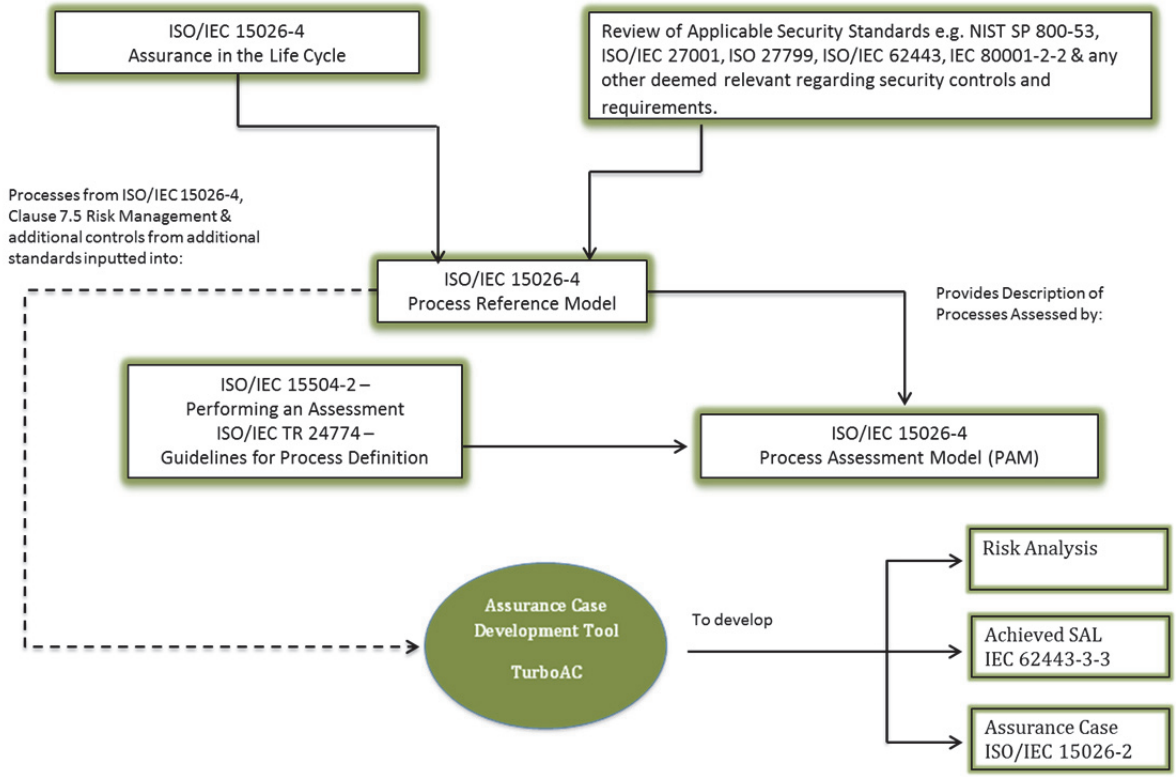

Figure 1: Research approach.

and a product point of view.

Developing a model to assess the Medical Device Manufacturer's development process maturity coupled with guidance for the establishment of a security assurance level addresses development and output. The product output is the medical device achieved security assurance level (SAL-A) reflecting the security capabilities for that device and also the security controls incorporated. This output, in the form of a security assurance case, will be the communication from Medical Device Manufacturers to Healthcare Delivery Organisations prior to acquisition. Managing the lifecycle process and the product security capability between the Medical Device Manufacturer and the Healthcare Delivery Organisation would greatly improve the current processes in the industry at the moment. Currently there is no methodology to address both the development processes and the product capabilities for security in medical devices. This is the primary focus of this research.

Hence, it is envisaged that the output of this research will positively impact the medical device domain by building awareness of security vulnerabilities, threats and related risks between the Healthcare Delivery Organisation and the Medical Device Manufacturer.

ACKNOWLEDGEMENTS

This research is supported by the Science Foundation Ireland (SFI) Stokes Lectureship Programme, grant number 07/SK/I1299, the SFI Principal Investigator Programme, grant number 08/IN.1/I2030 (the funding of this project was awarded by Science Foundation Ireland under a co-funding initiative by the Irish Government and European Regional Development Fund), and supported in part by Lero - the Irish Software Engineering Research Centre (http://www.lero.ie) grant 10/CE/I1855.

REFERENCES

DHS 2012. Attack Surface: *Healthcare and Public Heath Sector*.

Fergal McCaffery & Dorling, A. 2010. *Medi SPICE Development. Software Process Maintenance and Evolution: Improvement and Practical Journal*. 255-268.

Goodenough, J., Lipson, H. & Weinstock, C. 2012. *Arguing Security - Creating Security Assurance Cases*.

Government Accountability Office 2012. Medical Devices, FDA Should Expland Its Consideration of Information Security for Certain Types of Devices. In: GAO (ed.).

IEC 2010. IEC/TR 24774 *Systems and software engineering. Life cycle management. Guidelines for process description*.

IEC 2011a. IEC 62443-3-3 Ed. 1.0, Security for industrial automation and control systems - Network and system security.

Part 3-3: *System security requirements and security assurance levels Introductory Note. International Electrotechnical Committee*.

IEC 2011b. IEC/TR 80001-1 - Application of risk management for IT-networks incorporating medical devices.

IEC 2011c. IEC/TR 80001-2-2 Ed. 1.0 - Draft Technical Report - Application of risk management for IT-networks incorporating medical devices. *Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls. International Electrotechnical Committee.*

IEEE 2011. ISO/IEC 15026-2: 2011 Systems & Software Engineering, Systems & Software Assurance, Part 2: Assurance Case.

ISO 2008. EN ISO 27799:2008 Health informatics. Information security management in health using ISO/IEC 27002.

ISO/IEC 2003. ISO/IEC 15504-2: 2003 Software Engineering - Process Assessment - Performing an Assessment.

ISO/IEC 2005. ISO/IEC 27002:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management.

ISO/IEC 2006. ISO/IEC 15504-5: 2006 Information technology — Process Assessment — Part 5: An exemplar Process Assessment Model.

NIST 2009. 800-53 Recommended Security Controls for Federal Information Systems and Organisations. In: COMMERCE, U. S. D. O. (ed.) Revision 3 ed.

SEI 2010. *CMMI-DEV, CMMI for Development.*